



SIPP 3.3 Stack-Based Buffer Overflow via Configuration File

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2018-25225
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-28 12:16:03 UTC
Updated	2026-04-08 19:36:28 UTC
Description	SIPP 3.3 contains a stack-based buffer overflow vulnerability that allows local unauthenticated attackers to execute arbitrary code.

Risk And Classification

Primary CVSS: v4.0 8.6 HIGH from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000280000 probability, percentile 0.080410000 (date 2026-04-13)

Problem Types: CWE-306 | CWE-306 Missing Authentication for Critical Function

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
4.0	CNA	CVSS	8.6	HIGH	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	disclosure@vulncheck.com	Secondary	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	8.4	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X



CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H



NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sipp Project	Sipp	3.3	All	All	All

Vendor Declared Affected Products

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Sipp	SIPP	affected 3.3	Not specified
References				
Reference	Source	Link	Title	
sipp.sourceforge.net	disclosure@vulncheck.com	sipp.sourceforge.net	Pi	
www.exploit-db.com/exploits/45288	disclosure@vulncheck.com	www.exploit-db.com	E:	
www.vulncheck.com/advisories/sipp-stack-based-buffer-overflow-via-configuration...	disclosure@vulncheck.com	www.vulncheck.com	TI	
CVE Program record	CVE.ORG	www.cve.org	cæ	
NVD vulnerability detail	NVD	nvd.nist.gov	cæ	
Vendor Comments And Credit				
Discovery Credit				
CNA: Juan Sacco <jsacco@exploitpack.com> - http://exploitpack.com (en)				
There are currently no legacy QID mappings associated with this CVE.				